Trusted Distribution Plan

DOCUMENT IDENTIFIER: A-SP-ELMF753-00-0000 Rev B, 01-May-1992

ABSTRACT: This document provides the plan for trusted distribution of Digital products. The document includes discussions of the distribution systems used to provide trusted distribution for Trusted Computing Base (TCB) components.

APPLICABILITY: This plan mandates individual accountability of all personnel involved with handling each individual shipment in a trusted fashion.

STATUS: APPROVED 01-May-1992; use VTX SMC for current status.

© Digital Equipment Corporation, 1992. All rights reserved.
Unpublished - rights reserved under the copyright laws of the United States

The drawings and specifications contained in this document are the property of Digital Equipment Corporation, and may not be reproduced, copied, used or disclosed, in whole or in part to persons other than employees of Digital Equipment Corporation without written permission from Digital Equipment Corporation.

Disclosure by Digital Equipment Corporation to the National Computer Security Center is made pursuant to the terms and conditions of the CMW Contract MDA908-88-C-1187, signed June, 1988.

Trusted Distribution Plan

DOCUMENT IDENTIFIER: A-SP-ELMF753-00-0000 Rev B, 01-May-1992

REVISION HISTORY:	Rev A	17-Jun-1991	
	Rev B	01-May-1992	ECO Number NRO01

Document Management Category:	Manufacturing Plant Operations (MPO)
Responsible Department:	Government Systems Group
Responsible Person:	Barbara Thomson

APPROVAL: This document has been reviewed and approved by the General Review group for its category.

Barbara Thomson - Government Systems Group

Direct requests for further information to:

Barbara Thomson
Use $ VTX ELF for the latest location information.

Use VTX SMC to order copies of this document from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

The DIGITAL logo is a trademark of Digital Equipment Corporation.

CONTENTS

Preface v

1 Overview 1
1.1 TRUSTED DISTRIBUTION APPROACH 1
1.2 TCB ELEMENTS 2

2 SALES AND ADMINISTRATION PLAN 2
2.1 SALES CHANNELS 2
2.2 PRODUCT DELIVERABLES 3
2.2.1 Trusted Distribution for Systems 3
2.2.2 Trusted Software Distribution 4
2.2.3 Trusted Distribution for Add-on Hardware 4
2.2.4 Digital Maintenance of TCB Hardware 4

3 TRUSTED DISTRIBUTION 4
3.1 DIGITAL SERVICES 4
3.1.1 Order Administration Procedures 5
3.1.2 Shipping Procedures 6
3.1.3 Audit 6
3.2 CONSTANT SURVEILLANCE COURIERS 7
3.2.1 USPS Registered Mail 7
3.2.2 Courier Security and Accountability Controls 8
3.3 HARDWARE MAINTENANCE TRUSTED DISTRIBUTION 8
3.3.1 Digital's Maintenance Contracts 8
3.3.2 Security Controls 9

4 ABBREVIATIONS 9

5 TRUSTED DISTRIBUTION WORKING GROUP 10

Appendix A REFERENCED DOCUMENTS 11

A.1 Other Documents 11

A.2 Ordering Information 11

Preface

The Compartmented Mode Workstation (CMW) product must meet the requirements for trusted distribution under the *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for DoD5200.28-STD* and the *Security Requirements for System High and Compartmented Mode Workstations, Revision 1 DDS-2600-5502-87*.

This document describes the proposed plan for supporting trusted distribution and supersedes all prior discussions. The plan was developed by the Secure Systems Group and the Government Systems Group in conjunction with the several Digital organizations that will be responsible for the implementation of this plan. The document is being submitted to the National Computer Security Center as part of the developmental evaluation for the Compartmented Mode Workstation product and various Digital organizations for approval and implementation planning.

1 Overview

This document provides the plan for offering trusted distribution of Digital products. The document includes discussions of the distribution systems used to provide trusted distribution for Trusted Computing Base (TCB) components, the assurance mechanisms employed for each distribution system, and coverage of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) requirement. The trusted distribution requirement, as specified by the TCSEC, is cited here for reference.

"A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies." [Depa85, p. 106]

The National Computer Security Center's *A Guide to Understanding Trusted Distribution in Trusted Systems, NCSC-TG-008, Version 1*, states:

"There are basically two threats that trusted distribution protects against. The first is the threat of someone tampering with a system during its movement from a vendor site to a customer site ... The second threat ... is that the TCB is a counterfeit; that is the system or update did not come from the vendor site." [Nati88]

1.1 TRUSTED DISTRIBUTION APPROACH

Digital protects against the threat of someone's tampering with trusted distribution shipments by using:

- United States Postal Service (USPS) registered mail, or
- Constant surveillance couriers

Digital trusted distribution protects against the threat of modification of the shipment before it is picked up for delivery to the customer by not associating the customer's name and address with the order until it is placed in the hands of the USPS or the courier.

Digital trusted distribution protects against the threat of a counterfeit shipment by separately notifying the customer of an impending USPS registered mail or commercial courier shipment using the unique shipment identification and estimated time of arrival *(ETA)*.

Constant surveillance couriers provide assurance that TCB components have been handled only by authorized personnel while in transit between Digital and the customer's site. Digital will monitor commercial shipments of TCB components for anomalous conditions that may indicate security violations. The accountability controls provide individual accountability of all personnel involved with handling each shipment in the trusted distribution system. Audit trails support analysis, which can identify potential security problems, and support tracing of any security problems.

1.2 TCB ELEMENTS

Trusted distribution maintains the integrity of the current TCB software, firmware, and hardware as well as any updates made to them. The CMW TCB consists of the elements listed here.

HARDWARE (including FIRMWARE)

- Workstation system box, including its board-level components, such as logic modules, memory boards and controllers
- Keyboard, monitor and mouse
- Hardware documentation manuals

SOFTWARE

- CMW kernel software distribution media
- CMW documentation manuals

UPDATES

- Hardware modules, including those containing the firmware ROMs
- CMW kernel software update distribution media
- Documentation update manuals

Digital packaging for all hardware, software, and documentation TCB components conforms to internal Digital standards and specifications that meet or exceed local and international regulations, and common carrier and USPS shipping requirements and standards. This includes, as a minimum, but is not limited to, such standards as the *Uniform Freight Classification, Rule 41 (US)*, and in particular, Section 7 which specifies carton closures. Furthermore, the given TCB components are packaged according to Digital's internal standards for shipping products internationally, which includes, but is not limited to, requirements for protection from moisture, such as plastic bags for individual components, and shrink wrap for individual documents, in addition to stringent standards for external consolidation packaging.

2 SALES AND ADMINISTRATION PLAN

2.1 SALES CHANNELS

All Digital products and services, shipped by way of trusted distribution will be sold through the Digital direct sales force and Digital telemarketing. Orders for trusted distribution will be processed through the standard Digital order administration system. Customers who require trusted distribution must so designate on the purchase order.

As with all Digital products, transportation of orders from Digital to the customer's site shall be the customer's responsibility. Digital will offer trusted distribution as an added-cost option for customers who prefer not to provide transportation themselves.

2.2 PRODUCT DELIVERABLES

Digital will offer the TCB in the following ways:

- As entire systems that include the entire TCB and desired customer options
- As a software product for a customer's installed systems
- As an update service for the customer's software
- As add-on hardware options, such as add-on memory and new controllers
- As service maintenance contracts for the customer's hardware

Each way is discussed further, with the trusted distribution delivery approach.

2.2.1 Trusted Distribution for Systems

Systems that include the entire hardware, firmware, and software in the Trusted Computing Base (TCB) will be available for sale. To ensure these systems arrive at the customer's site meeting the trusted distribution criteria, Digital shall enable the customer to request Digital to ship their systems by a courier or by USPS registered mail.

If the systems order does not meet the USPS requirements for shipping by registered mail, Digital shall ship the order by a courier. For courier shipments, Digital shall:

1. Require that the courier provide a constant surveillance service.
2. Require that the courier provide insurance on the customer's behalf for the safety of the shipment.
3. Notify the customer's designated consignee, at least 24 hours before the estimated time of arrival, what Digital is shipping, how Digital is shipping it, and when the shipment is expected to arrive.

By protecting the identity of the customer during order fulfillment to prevent targeting the order components, Digital provides assurance that the TCB is not modified before the courier picks up the shipment.

If the system order meets the USPS requirements for shipping registered mail, then Digital shall proceed as follows:

1. Package the shipment to meet the requirements of registered mail, which includes enclosing the material in opaque containers and sealing the seams and edges.
2. Notify the customer's designated consignee, at least 24 hours before the estimated time of arrival, by a method other than U.S. mail, to ensure the identity of the sender and what Digital is shipping, how Digital is shipping it, and when the shipment is expected to arrive.
3. Provide assurance that TCB is not modified before the USPS picks up the shipment by protecting the identity of the customer during order fulfillment to prevent targeting the order components.

2.2.2 Trusted Software Distribution

Customers who purchase initial copies of CMW software separately from the system (that is, as software-only orders), or who purchase software update contracts, can request trusted distribution of that software.

Digital treats initial shipment of add-on software and software updates in the same manner as system shipments. The software trusted distribution method is to deliver the software to the customer by USPS registered mail or courier.

It is the customer's responsibility, when placing an order for add-on software or for a software update service contract, to specify that TCB parts are to be shipped by trusted distribution.

2.2.3 Trusted Distribution for Add-on Hardware

Customers who purchase hardware components of the TCB from Digital to increase the system capabilities, or to service their systems when they are on a self-maintenance program, can request trusted distribution of those parts.

Digital treats shipment of add-on hardware and self-maintenance hardware updates in the same manner as system shipments. The method for trusted distribution of hardware components is to deliver the components to the customer by USPS registered mail or courier.

It is the customer's responsibility, when placing an order for add-on or self-maintenance update hardware, to specify that the TCB parts are to be shipped by trusted distribution.

2.2.4 Digital Maintenance of TCB Hardware

Digital shall enable customers to request trusted distribution with Digital's standard hardware maintenance service.

Digital's service personnel take precautions to ensure that shipment of replacement parts, when necessary, is consistent with trusted distribution goals.

Authorized Digital service personnel order the replacement parts and hand deliver them to the customer's site.

It shall be the customer's responsibility to determine the level of trust that the customer requires of the Digital service personnel, who are assigned to service the customer's system, based on the customer's determination of the level of sensitivity of the data that the system will process.

3 TRUSTED DISTRIBUTION

3.1 DIGITAL SERVICES

Digital customers may request the trusted distribution service in conjunction with the purchase of products or product update services.

With the exception of hardware maintenance contracts, Digital uses the services of the USPS or a commerical courier to deliver TCB components to the customer.

Digital augments the services of the USPS or commercial courier with the following services:

1. *Order Confirmation* — Send a separate order confirmation to the customer when the order fulfillment begins. The order confirmation identifies the individual order components by type.
2. *Targeting Protection* — Keep an order's destination anonymous to those handling and warehousing the order until the order is picked up.
3. *ETA Notification* — Notify the customer of the ETA of a shipment when the order is ready to leave Digital's dock.
4. *Unique Shipment Identification* — Notify the customer, by an alternate means, of the unique identifier (for example, waybill number or registered mail registration number) for the shipments that leave Digital's dock, to assure the customer of the identity of the sender.
5. *Inventory* — Include a bill of materials, initialed by the packers, with the shipment for inventory cross-check against the order confirmation when the shipment arrives.
6. *Separate Invoicing* — Send an invoice to the customer by alternate means.
7. *Receipt Confirmation* — Confirm the customer's receipt of a shipment by verifying the paperwork received by the customer independently of the USPS or a commercial courier, whichever delivers the shipment.

3.1.1 Order Administration Procedures

When a customer places an order, the Customer Administration Services (CAS) representative enters it into an order administration system. These systems, and the software update and hardware maintenance service contract systems, route the order to the appropriate order fulfillment systems. The order fulfillment systems, in turn, schedule manufacturing personnel to ship the order components from their order fulfillment locations to a consolidation center.

All these systems are protected from general access. Only authorized Digital users are permitted access to these systems, on an individually restricted basis.

For trusted distribution orders, Digital shall protect the customer's identity during order fulfillment to prevent targeting of the customer's TCB order. Only the customer's local Digital sales representative, local CAS representative, service contract supervisor, Digital's lead shipper handling the order at the consolidation dock, and their supervisors or authorized representatives, as appropriate, shall have access to the customer's real name and address during order fulfillment.

The customer's real name and address shall be classified as DIGITAL CONFIDENTIAL information. Only those identified earlier in this subparagraph shall have access to the information, and they shall treat it according to the Digital Corporate Security Policy for Information Protection. The policy defines DIGITAL CONFIDENTIAL information as that which must be restricted to access by only those persons within the company with a need to know. The information can be entered into a computer system, but access controls must be maintained on that information by the system on a user-by-user basis. Paper output that contains that information must be stored in locked desks, file cabinets, or rooms. If the information on paper is discarded, it must be shredded or placed in locked collection boxes which are periodically emptied into shredders or incinerators. Similarly, magnetic

media must also be kept in locked storage and thoroughly degaussed or written over to destroy data written thereon.

At no time shall the customer's real name and address appear on, in, or near the components used to fulfill the order, or on paperwork associated with those components as they move through or between order fulfillment sites.

3.1.2 Shipping Procedures

All the items in a trusted distribution order arrive at the consolidation center already boxed, sealed, and ready to ship. Digital shall not have the real name of the customer or the address attached to the items.

In the case of system or hardware orders, once all the items comprising an order arrive at the consolidation center, the Digital shipper obtains the customer's real name and address and prepares the paperwork for the shipment. Only the waybill or equivalent ship paperwork actually associates the items in the order with the customer's real name and address. The courier, under the supervision of the Digital shipper, then picks up the shipment from the Digital dock. The shipper then gives the courier the ship paperwork.

In the case of orders for software only or software updates, the packer seals the components of the order in a box or boxes, as necessary, for shipment by registered mail. At this point, the customer's real name or address does not appear in or on the box. When the shipper receives the box or boxes on the shipping dock, the shipper obtains the customer's real name and address and prepares the ship paperwork. The USPS, under the supervision of the Digital shipper, then picks up the packages, as defined in the USPS regulations for registered mail.

All Digital manufacturing facilities and warehouses are restricted to access by authorized Digital employees only. All visitors to Digital plants require escorts, and even while escorted, are restricted from entering manufacturing floors and shipping docks except in special traffic lanes.

3.1.3 Audit

When the designated customer consignee receives the shipment, the customer shall be responsible for verifying the unique shipment identification that accompanies the shipment against that received from Digital by alternate means. The customer shall be responsible for returning a copy of that shipment paperwork to Digital by alternate means.

In addition, as in the normal course of business, it shall be the customer's responsibility to verify that what was shipped was indeed what the customer ordered. The customer receives an order confirmation (*Order Acknowledgement*) directly from the customer's local Digital CAS representative. The order confirmation is generated by the order adminstration system and sent prior to order fulfillment. The order acknowledgement form identifies the order number, the items, quantities, model numbers, and scheduled ship dates for each of the items ordered. Shortly before the order ships, the Digital shipper contacts the customer *(ETA Notification)* and provides the unique shipment identification for the order, number of pieces in the order, carrier identification, and expected arrival time. When the shipment arrives, the customer receives the shipper's waybill and/or carrier manifest, and Digital's bill of lading, with the unique shipment identification *(Carrier Number)*, or, in the case of USPS registered mail shipments, the restricted delivery receipt(s) and the unique registration number(s). The customer also receives, but is not limited to receiving, the

internally packaged bill(s) of materials and/or content listings, and, with system shipments, a separate content listing *(Product Delivery Document)*. These lists cross-identify the order number, the items, quantities, and model numbers that correspond to those in the order acknowledgement form.

When the customer sends a copy of the ship paperwork to Digital, the Digital shipper shall again verify that the copy matches the paperwork that was sent with the shipment.

Digital shippers consolidate and maintain audit information from the shipping records, including bills of lading, waybills, and product delivery documents, that identify the packers, drivers, lead shippers, receivers, and customer security representatives for each shipment. The information comes from multiple sources, thereby allowing correlation and verification of the audit records.

In addition to providing information on variances in performance between different drivers and carriers, the audit records provide information that can be used to isolate anomalous behavior (as compared to past performance) on the part of individual drivers. Customer security representatives will be able to contact the Digital shippers to access the audit records.

3.2 CONSTANT SURVEILLANCE COURIERS

Based on the size and destination of the order, the Digital shipper determines the most appropriate trusted distribution method from the list of approved alternatives. The list includes:

- United States Postal Service registered mail
- Constant surveillance couriers

Shipments of the TCB components will be delivered in a manner that allows continual surveillance and monitoring during transit as well as assurance of the trusted shipment at the delivery site.

Also, if the customer wishes special services from a courier on the approved list, the customer may request that courier and those services when placing the order with the Digital CAS representative.

NOTE

It shall be the customer's responsibility to provide Digital with the required forms, for example, if the customer requests a DoD CSS Signature and Tally Record (DD Form 1907), that Digital shall in turn furnish to the courier for the shipment.

3.2.1 USPS Registered Mail

The USPS provides a unique registration number for each package sent by registered mail. The package is labelled with its registration number and stamped with the time and place of origin. The carrier also stamps each taped seam so that it can be determined if the package has been tampered with. The package is kept in a locked cage or pouch while in transit or storage. Each post office employee handling the package logs it on a handling record maintained at that office. The *United States Postal Service, Domestic Mail Manual and International Mail Manual* states: *"Registered mail is the most secure service the U.S. Postal Service offers. It incorporates a system of receipts to monitor the mail's movement from the point of acceptance to delivery."* [Unit90 D, p. 571]

Digital shall require restricted delivery for registered mail. Only the named customer may receive the mail. Digital shall insure domestic registered mail and require a return receipt, unless the customer requests otherwise. Digital shall notify the customer, by an alternate means, of the expected delivery of registered mail, using the registration number or numbers for the shipments. It shall be the customer's responsibility to return a copy of the packaging registration to Digital by separate means. Digital shall verify that the registration matches that of the shipment sent to the customer.

3.2.2 Courier Security and Accountability Controls

It shall be the customer's responsibility to determine the level of trust that Digital shall require of the courier, based on the customer's determination of the level of sensitivity of the data that the system will process. Unless otherwise requested by the customer, Digital shall require that the couriers meet the Department of Defense criteria for constant surveillance service couriers, as documented in the *Uniform Tender of Rates and/or Charges for Transportation Services, Tender No.7C Appendix B, Page 1*. [Mili89]

The security criteria for freight carriers, other than the USPS, that Digital has established are as follows:

- Physically separate and secure trusted parcels from normal shipments.
- Constantly attend trusted parcels.
- Individual accountability for parcels while in transit.
- Bonded drivers.
- Provide customer-signed trusted acknowledgement upon delivery.

The accountability criteria that Digital has established for freight carriers, other than the USPS are as follows:

- Ability to monitor parcel status and location by authorized individuals.
- Carrier signature sheet with the signature of the responsible shipper detailing all transfers of parcels while on route.

3.3 HARDWARE MAINTENANCE TRUSTED DISTRIBUTION

Customers may choose to have Digital provide maintenance for the hardware, or they may choose to maintain their systems themselves. In both cases, maintaining systems involves replacement of defective parts and installation of corrections to hardware, known as Field Change Orders (FCOs).

Self-maintenance customers may order their replacement parts under trusted distribution, as previously discussed. The following paragraphs describe the trusted distribution procedures for hardware update contract customers.

3.3.1 Digital's Maintenance Contracts

Digital's standard hardware maintenance service provides a means for trusted distribution. Replacement parts are hand delivered to the customer site by authorized Digital service personnel. FCOs to the hardware are delivered to customers using these maintenance service delivery methods.

3.3.2 Security Controls

Trusted distribution is accomplished through internal security procedures.

The steps that a Customer Service Engineer (CSE) will take to service a system are as follows:

1. Is the customer under a Trusted Distribution contract?
   - If yes, go to 2. If no, no special actions are required.
2. Is the customer's problem related to the list of TCB components?
   - If yes, go to 3. If no, no special actions are required.
3. Pick up the service kit or kits from the CSE's Service Delivery Unit (SDU), and go directly to the customer site without leaving the material unattended at any time. Proceed to 4.
4. Is the material available from the kit brought to the customer site?
   - If yes, install the required part; no further special actions are required.
   - If no, go to 5.
5. Place a priority order for the material to be shipped to the SDU. Once the replacement part is received at the SDU, go to 6.
6. Pick up the replacement part from the SDU and go directly to the customer site without leaving the part unattended at any time.

Precautions are taken to ensure that expedited shipment of replacement parts, when necessary, is consistent with trusted distribution goals.

Material ordered from Digital's warehouses is not assigned to a particular customer. Parts are shipped to the CSE's SDU where they are then picked up by the responsible Customer Service Engineer.

Material is only assigned to a particular customer when it is picked up from the SDU by the Service Engineer. From that point on, the material is always attended by the Service Engineer or other authorized Digital personnel until installation at the customer site.

Inventory at all stocking locations is under restricted access.

4 ABBREVIATIONS

The abbreviations used most frequently throughout this document are listed in the following table.

Abbreviation	Definition
CAS	Customer Administration Services
CMW	Compartmented Mode Workstation
CSE	Customer Service Engineer
CSS	Constant Surveillance Service
DoD	Department of Defense
ETA	Estimated Time of Arrival

Abbreviation	Definition
ROM	Read-Only Memory
SDU	Service Delivery Unit
TCB	Trusted Computing Base
TCSEC	Trusted Computing Systems Evaluation Criteria
USAD	Digital United States Area Distribution
USPS	United States Postal Service

5 TRUSTED DISTRIBUTION WORKING GROUP

The individual contributors to this trusted distribution pland and their groups are listed here for your information. That is followed by a list of external documents that were used as reference material to prepare this document.

- Scott Almeida, Customer Service Group Logistics
- Patrick Deyo, Software Supply Business
- Monte Dickey, Government Security Consultant
- Jay Ellowitz, U.S. Manufacturing Business Center
- Barbara Farnsworth, Order Management System
- Roger Kipp, Eastern U.S. Area Distribution
- Lou Nay, Customer Services Systems Engineering
- Ron Santos, U.S. Customer Distribution
- Barbara Thomson, Government Systems Group

APPENDIX A REFERENCED DOCUMENTS

For informational purposes, the reference numbers used in text correspond to the document numbers listed here.

A.1 Other Documents

Document Number	Document Title
DEPA85	*Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard, DOD 5200.28-STD, December 1985*
MILI89	*Uniform Tender of Rates and/or Charges for Transportation Services, Tender No. 7C, Center No. 141047, May 1989, Military Traffic Management Command, Directorate of Inland Traffic, Falls Church, VA 22041-5050*
NATI88	*A Guide to Understanding Trusted Distribution in Trusted Systems, National Computer Security Center, NCSC-TG-008, Version 1, December 1988*
	Security Requirements for System High and Compartmented Mode Workstation
	Uniform Freight Classification, Rule 41 (U.S.), Section 7.
UNIT90	*United States Postal Service, Domestic Mail Manual and International Mail Manual, June 1990. Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402-9371*

A.2 Ordering Information

Copies of these documents may be acquired by contacting Compartmented Mode Workstation Engineering (CMW), Government Systems Group, MKO2-1/K06.

Following are the sources for documents not available from Standards and Methods Control.

- Federal Standards, Military Standards, Naval Publications, and Forms Center,
  5801 Tabor Avenue
  Philadelphia, PA 19120
  Telephone (215) 697-3321
- Superintendent of Documents,
  U. S. Government Printing Office
  Washington, DC 20402-9371

```
+---------------------------------------------------------------------+
|                        READER COMMENTS                              |
|                                                                     |
| Your  comments  and suggestions  will help  Standards and Methods   |
| Control improve their services and documents.                       |
+---------------------------------------------------------------------+
```

Did you request this document? _____ If so, did it arrive within a satisfactory period of time? _____ Please comment.

What are your impressions of this document? Consider format, organization, completeness, readability, and illustrations.

————————————**FOLD ON THIS LINE**———————————————————————— -

Did you find technical or clerical errors in this document? If so, please specify the page number(s) and the error(s).

Are the instructions for the update package clear? _____
Was an index available? _____ If not, is one needed? _____
Do you have other suggestions for improving this document?

The following information is optional:

Name _____ Mailstop _____

Department _____ Node _____

Send your comments to JOKUR::PROJECTS, or fold, staple, and send this page through interoffice mail to:

```
+------------------------------+
|       READERS' COMMENTS      |
| STANDARDS AND METHODS CONTROL |
|           NRO4/D4            |
+------------------------------+
```